BITTORRENT RESOURCE DISCOVERY VIA THE NOSTR PROTOCOL

Study of the NIP-35 standard and the "Web of Trust" as alternatives to centralized indexers

gmonarque

December 29, 2025

Abstract

This document explores the use of the Nostr protocol and its specification **NIP-35** (Torrents) as a discovery layer for the BitTorrent network. It analyzes how this standard, coupled with a **delegated curation** mechanism (Web of Trust), ensures the quality and authenticity of metadata without resorting to centralized moderation. Finally, it presents the **lighthouse** project, a proof of concept (PoC) making this new paradigm accessible to end users.

1 Context

The BitTorrent protocol is technically mature for data transport (the file), but offers no native mechanism for content search and indexing. Historically, this gap has been filled by indexing websites.

This centralized approach presents a major friction: the user must trust a single site to moderate content. If this site shuts down, discovery capability disappears, even though the underlying BitTorrent network remains functional.

2 The technical solution: Nostr and NIP-35

The Nostr protocol offers an architectural alternative by acting as a global and censorship-resistant message bus. The **NIP-35** specification allows encapsulating file metadata (name, hash, magnet link, etc.) in a cryptographically signed event.

However, an open and censorship-resistant network poses an immediate challenge: spam and data pollution. This is where the fundamental concept of the **Web of Trust** comes in.

3 The trust model (Web of Trust)

The major innovation lies not only in data transport, but in reputation management. The architecture replaces centralized moderation (one admin validates everything) with distributed curation.

This model revolves around three actors:

3.1 1. The Emitter (the source)

The uploader no longer registers on a platform. They generate a cryptographic key pair. Each post is signed with their private key. This signature mathematically guarantees that the file indeed comes from the claimed author (e.g., an archiving group, a software publisher), preventing any identity theft.

3.2 2. The Curator (the human filter)

This is the essential link for discovering quality content.

- **Role:** The curator is a trusted third party (expert, enthusiast, organization) who performs a selection task. They do not necessarily store the files but publish and maintain a list of public keys (a *Follow List*) corresponding to emitters they have verified and validated.
- **Diversity:** There can be an infinite number of specialized curators (e.g., a "Classic Cinema" curator, a "Linux ISOs" curator, a "Free Music" curator).
- **Responsibility:** If an emitter starts publishing corrupt files, the curator removes them from their list, instantly sanitizing the feed for all their subscribers.

3.3 3. The User (the beneficiary)

The end user no longer needs to search through the noise of the global network. They subscribe to the curators of their choice.

- **Transitivity of trust:** The client software applies the following logic: *"I trust curator A. Curator A validates emitter B. Therefore, my software indexes and displays content from B."*
- **Sovereignty:** The user builds their own recommendation algorithm by choosing their trusted sources. They are protected from spam because they index only what is validated by their web of trust.

4 Proof of concept

While the Nostr protocol provides the infrastructure and cryptography, a tool is missing to make these abstract concepts usable by the general public.

The open-source project **lighthouse** was developed to bridge this gap. It acts as a **local indexing client** that implements this Web of Trust logic.

It operates as follows:

1. **Targeted aggregation:** It connects to the Nostr network but scrapes only events validated by curators followed by the user.
2. **Structuring:** It organizes this metadata into a searchable local database (Search, Categories, Covers).
3. **Interoperability:** It exposes this data via a standard API (Torznab), allowing existing automation software (Sonarr, Radarr, *arr) to interact with this decentralized network exactly as if it were a classic tracker.

5 Conclusion

The integration of the NIP-35 standard coupled with the delegated curation mechanism represents a possible evolution of the BitTorrent ecosystem. By technically separating file storage, metadata publication, and trust validation, this model offers resilience and longevity that centralized web indexers technically cannot guarantee.